

Vorlage ULD-SH – Stand: Januar 2022

Achtung: Diese Texte sind für den jeweiligen Sachverhalt auszuwählen und ggf. anzupassen.

Im Rahmen einer Beschwerde/Kontrollanregung wurde ich auf Ihre Website/App

_____ .de

und die im Zusammenhang damit stehenden Datenverarbeitungsvorgänge hingewiesen.

Die Beschwerde/Kontrollanregung richtet sich insbesondere dagegen, dass auf Ihrer Website/ in Ihrer App sogenannte Cookies gesetzt werden, ohne dass die dadurch stattfindende Verarbeitung personenbezogener Daten auf einer hierzu hinreichenden Rechtsgrundlage basiere, und dass die im Zusammenhang mit der Verarbeitung entstehenden Pflichten der DSGVO, wie z. B. die Informationspflichten nach Art. 13 DSGVO, nicht eingehalten würden.

1. Zur Verwendung von Cookies

Bezüglich der Nutzung von Cookies und anderen sogenannten Tracking-Technologien verweise ich auf die „Orientierungshilfe der Aufsichtsbehörden für Anbieter:innen von Telemedien ab dem 1. Dezember 2021“ der Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder, die unter der Adresse:

https://www.datenschutzkonferenz-online.de/media/oh/20211220_oh_telemedien.pdf

abrufbar ist. Hieraus:

„Die Abfrage einer Einwilligung erfolgt in der Praxis regelmäßig dadurch, dass beim ersten Aufruf einer Webseite oder einer App ein Banner oder ähnliches grafisches Element mit Schaltflächen angezeigt wird. Über den Einsatz von Cookies und ähnlichen Technologien hinaus wird mit solchen Einwilligungsbannern jedoch meist auch eine Einwilligung für nachfolgende Datenverarbeitungsprozesse abgefragt.“

Weiter:

*„Die Einwilligung in das Speichern und Auslesen von Informationen, die nach § 25 Abs. 1 TTDSG erforderlich ist, und die Einwilligung, die als Rechtsgrundlage für eine geplante weitere Verarbeitung der ausgelesenen Daten gemäß Art. 6 Abs. 1 lit. a DS-GVO erforderlich sein kann, können unter Berücksichtigung der nachfolgenden Bedingungen **durch dieselbe Handlung** erteilt werden. [...] Hierbei ist darauf zu achten, dass bei der Abfrage **eindeutig erkennbar sein muss**, dass mit einer einzelnen Handlung, bspw. dem Betätigen einer Schaltfläche, **mehrere Einwilligungen** erteilt werden. Werden Nutzende, z. B. mittels eines **Banners**, auf einer Webseite darum gebeten, eine Einwilligung in den Einsatz von Cookies zu erteilen, ohne dass im Wortlaut der Einwilligung auch die Folgeverarbeitungen angesprochen werden, so handelt es sich nicht um eine gebündelte Einwilligung nach TTDSG und DS-GVO, sondern lediglich um eine Einwilligung nach dem TTDSG.“*

Hinsichtlich der Anforderungen an derartige Einwilligungsbanner sind insbesondere folgende Anforderungen zu beachten:

„- Beim erstmaligen Öffnen einer Website oder App erscheint das Einwilligungsbanner beispielsweise als eigenes HTML-Element. In der Regel besteht dieses Element aus einer Übersicht aller einwilligungsbedürftigen Verarbeitungsvorgänge, die unter Nennung der beteiligten Akteure und deren Funktion ausreichend erklärt werden und über ein Auswahlmenü aktiviert werden können.“

Aktivieren bedeutet in diesem Zusammenhang, dass die Auswahlmöglichkeiten **nicht „aktiviert“ voreingestellt sein dürfen.**

- Während das Einwilligungsbanner angezeigt wird, werden zunächst keine weitergehenden Skripte einer Website oder einer App, die potenziell auf die Endgeräte der Nutzenden zugreifen (TTDSG) oder deren personenbezogene Daten verarbeiten (DS-GVO) und insbesondere auch keine Inhalte von fremden Servern geladen, soweit die damit verbundene Offenlegung personenbezogener Daten einer Einwilligung bedarf. Der Zugriff auf Impressum und Datenschutzerklärung darf durch das Einwilligungsbanner nicht behindert werden.

- Erst wenn Nutzer:innen ihre Einwilligung(en) durch eine aktive Handlung, wie zum Beispiel das Setzen von Häkchen im Einwilligungsbanner oder den Klick auf eine Schaltfläche abgegeben haben, dürfen Informationen auf den Endgeräten gespeichert oder aus diesem ausgelesen werden sowie die einwilligungsbedürftige Datenverarbeitung tatsächlich stattfinden.

- Den Nutzer:innen muss im Einwilligungsbanner eine gegenüber der Zustimmung gleichwertige Möglichkeit gegeben werden, die Einwilligung zu verweigern. Wenn es auf der ersten Ebene des Einwilligungsbanners eine Schaltfläche für eine Einwilligung in bestimmte Prozesse gibt, muss es dort auch eine entsprechend dargestellte Schaltfläche geben, um diese Prozesse abzulehnen.

- Die Abgabe der Einwilligung wird vom Verantwortlichen gespeichert, damit bei einem weiteren Aufruf der Website das Banner nicht erneut erscheint und die Einwilligung zu Nachweiszwecken gesichert ist. Zur Erfüllung der Nachweispflichten des Art. 7 Abs. 1 DS-GVO ist es gemäß Art. 11 Abs. 1 DS-GVO nicht erforderlich, dass die Nutzer dazu direkt identifiziert werden. Eine indirekte Identifizierung (vgl. Erwägungsgrund 26 der DS-GVO) ist ausreichend. In Fällen, in denen Nutzer keine Einwilligung abgeben, sollte dieser Umstand ohne Verwendung einer User-ID o. ä. auf den jeweiligen Endgeräten hinterlegt werden, um zu verhindern, dass eine erneute Aufforderung zur Abgabe einer Willenserklärung angezeigt wird.

- Da eine Einwilligung widerruflich ist, muss eine entsprechende Möglichkeit zum Widerruf implementiert werden. Der Widerruf muss so einfach möglich sein wie die Erteilung der Einwilligung, Art. 7 Abs. 3 S. 4 DS-GVO.“

In diesem Zusammenhang weise ich Sie auch auf das Urteil des Europäischen Gerichtshofs in der Rechtssache C-673/17 („Planet 49“) sowie die darauf aufbauende Entscheidung des Bundesgerichtshofs vom 28.05.2020 unter dem Aktenzeichen I ZR 7/16 hin, wodurch nochmals bestätigt wurde, dass es für eine Einwilligung einer eindeutig bestätigenden Handlung bedarf.

Der oben genannten Orientierungshilfe können Sie außerdem weitere Hinweise zur datenschutzkonformen Gestaltung eines Telemedienangebots entnehmen.

2. Zur Übermittlung personenbezogener Daten in einen Drittstaat

Verantwortliche haben zu prüfen, ob es bei einer Datenverarbeitung zu einer Übermittlung personenbezogener Daten in Drittländer kommt.

Ich weise Sie diesbezüglich auf das Urteil des EuGH in der Rechtssache C-311/18 (Schrems II) hin, wodurch der **Privacy-Shield-Beschluss der Europäischen Kommission 2016/1250 für ungültig erklärt wurde**. Nach Art. 46 DS-GVO gilt, dass, falls kein Beschluss nach Art. 45 Abs. 3 DSGVO vorliegt, ein Verantwortlicher oder ein Auftragsverarbeiter personenbezogene Daten an ein Drittland oder eine internationale Organisation nur übermitteln darf, sofern der Verantwortliche bzw. der Auftragsverarbeiter geeignete Garantien vorgesehen hat und sofern den betroffenen Personen durchsetzbare Rechte und wirksame Rechtsbehelfe zur Verfügung stehen. Die bloße Verwendung von Standardvertragsklauseln reicht hierzu nicht aus. Auch bei einer Verwendung der neuen EU-Standardvertragsklauseln ist eine Prüfung der Rechtslage im Drittland und zusätzlicher ergänzender Maßnahmen erforderlich.

Weitere Informationen dazu finden Sie unter:

- https://www.datenschutzkonferenz-online.de/media/pm/20200616_pm_schrems2.pdf
- https://edpb.europa.eu/sites/edpb/files/files/file1/20200724_edpb_faqoncjeuc31118_de.pdf
- https://edpb.europa.eu/system/files/2021-06/edpb_recommendations_202001vo.2.0_supplementarymeasurestransferstools_en.pdf
- https://edpb.europa.eu/system/files/2021-04/edpb-edpsjointopinion01_2021_sccs_c_p_de_1.pdf

3. Bezüglich der Verpflichtung, eine Datenschutzerklärung bereitzustellen

Gemäß Art. 13 Abs. 1 und 2 DSGVO bestehen für den Verantwortlichen im Falle der Erhebung personenbezogener Daten bei betroffenen Personen Informationspflichten. Diese Informationspflichten entstehen auch bei der Ansteuerung eines Webauftritts durch Nutzende (Besucherinnen oder Besucher der Website). In Webauftritten werden diese Pflichtinformationen häufig in „Datenschutzhinweisen“ oder „Datenschutzerklärungen“ aufgeführt.

Zu den Inhalten der Informationspflichten verweisen wir auf unsere Informationsbroschüre (dort insbesondere unter Punkt Nr. 6):

www.datenschutzzentrum.de/uploads/praxisreihe/Praxisreihe-4-Informationspflichten.pdf

4. Nachweis- und Rechenschaftspflicht

Nach Art. 5 Abs. 2 DSGVO sind Sie als Verantwortlicher verpflichtet, die Einhaltung der datenschutzrechtlichen Vorschriften nachweisen zu können (Rechenschaftspflicht). Nach Art. 32 DSGVO haben Sie unter Berücksichtigung des Stands der Technik, der Implementierungskosten und der Art, des Umfangs, der Umstände und der Zwecke der Verarbeitung sowie der unterschiedlichen Eintrittswahrscheinlichkeit und Schwere des Risikos für die Rechte und Freiheiten natürlicher Personen geeignete technische und organisatorische Maßnahmen zu treffen, um ein dem Risiko angemessenes Schutzniveau zu gewährleisten.

In diesem Zusammenhang halte ich es für zwingend erforderlich, bei der Bereitstellung von Webseiten eine HTTPS-Verschlüsselung einzusetzen, wenn personenbezogene Daten eingegeben werden können.

Die vorgenannten Punkte sind mir im Rahmen einer ersten Sichtung Ihrer **Website/App** aufgrund der diesbezüglichen **Beschwerde/Kontrollanregung** aufgefallen. Ich weise Sie darauf hin, dass eine eingehende Prüfung Ihrer **Website/App** auf die Vereinbarkeit mit der DSGVO und dem TTDSG noch nicht erfolgt ist.

Wir behalten uns vor, Ihren Webauftritt zu einem späteren Zeitpunkt nochmals daraufhin zu prüfen, ob die datenschutzrechtlichen Vorgaben ordnungsgemäß umgesetzt wurden.